

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 57-006952
(43)Date of publication of application : 13.01.1982

(51)Int.CI.

G06F 13/00
G11C 29/00

(21)Application number : 55-081157
(22)Date of filing : 16.06.1980

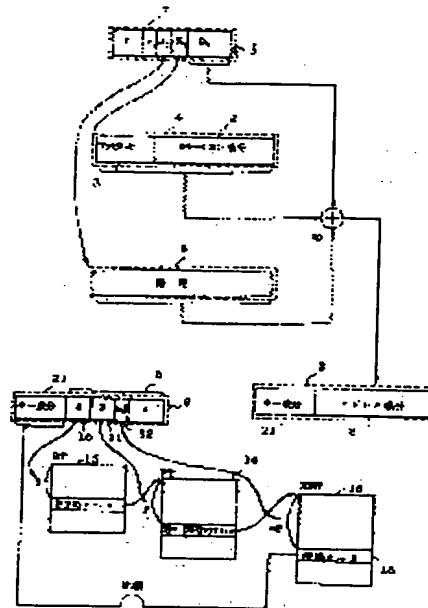
(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : UCHIYAMA KIMIAKI
KURATA MASAHIRO

(54) STORAGE PROTECTING SYSTEM

(57)Abstract:

PURPOSE: To ensure a strict limitation for the program range in which an access is allowed to the information and at the same time simplify the process during an access mode, by forming the base address with the location component and an access key.

CONSTITUTION: The base address is formed with a location component 2 and an access key 3, and a protective key 15 allotted to the storage region based on an address component 8 of an effective address 9. Then the key 15 is compared with a key component 21 shown in the address 9 to carry out a checking. For instance, a sum is obtained among the contents of a base register 4 designated by an instruction 7, the contents (deviation) of an index register 6 designated by the instruction 7 and a deviation 5 held in the instruction 7 in order to produce the address 9 of a subject of access. Then a control table XPT is prepared from the component 8 of the address 9 in reference to a segment table 13 and a page table 14, and the key 15 in the table XPT is compared with the component 21 to carry out a protection.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑯ 日本国特許庁 (JP)

⑮ 特許出願公開

⑰ 公開特許公報 (A)

昭57—6952

④ Int. Cl.³
G 06 F 13/00
G 11 C 29/00

識別記号

府内整理番号
7361-5B
6974-5B

⑩ 公開 昭和57年(1982)1月13日

発明の数 1
審査請求 未請求

(全 10 頁)

④ 記憶保護方式

⑤ 特 願 昭55—81157

⑥ 出 願 昭55(1980)6月16日

⑦ 発明者 内山公昭

横須賀市武1丁目2356番地日本
電信電話公社横須賀電気通信研

究所内

⑧ 発明者 倉田正博

横須賀市武1丁目2356番地日本
電信電話公社横須賀電気通信研
究所内

⑨ 出願人 日本電信電話公社

⑩ 代理人 弁理士 磯村雅俊

明細書

1. 発明の名称 記憶保護方式

2. 特許請求の範囲

記憶領域を区間に分割し、該区間にごとに保護キーを割り当てるとともに、該記憶領域にアクセスする命令がベース・アドレスの格納場所を指定するような情報処理装置において、該ベース・アドレスがロケーション成分とアクセス・キーで構成され、該ベース・アドレス内のロケーション成分および命令により指定された偏差成分から生成される実効アドレスのアドレス成分をもとにして、記憶領域に割り当てられた保護キーを得、該保護キーと、ベース・アドレスに示されるアクセス・キーとを比較チェックすることを特徴とする記憶保護方式。

3. 発明の詳細な説明

本発明は、情報処理装置における記憶保護方式について、特にアクセス・キー付きベース・アドレス記憶保護方式に関するものである。

情報処理装置において命令を実行する場合、記憶領域にアクセスが行われるまでの過程には、次の2つの段階がある。

第1の段階は実効アドレスの生成段階であつて、これは命令で指定されたレジスタ（アドレス修飾用のレジスタ）に格納されているアドレスと、偏差成分（命令中に保持される偏差（ディスプレイスメント）および命令で指定された修飾レジスタの内容）との和を算出し、アクセスの対象となる実アドレスを生成する。実アドレスが生成される場合、命令で指定されるアドレス修飾用のレジスタをベース・アドレス・レジスタと呼び、データの先頭アドレスを示す。

第2段階は、実記憶装置へのアクセス段階であつて、これは命令から生成された実効アドレスを記憶領域に付与された論理アドレスに対応づけ、アドレス変換機構を経て実記憶装置にアクセスする。

このようにして記憶領域にアクセスが行われるが、記憶領域に対する書き込みの制限、プログラム暴走を防止するための命令の実行の制限、お上

び機密情報を守るために読み出し制限のために、従来より記憶保護が行われている。

従来より、一般的に用いられている記憶保護方式はキー保護方式であつて、例えば記憶領域を2Kバイト単位に分割して、それぞれにキー情報を割り当て、一方、処理装置の状態を示すプログラム状態語（以下PSW）の中にもキーを設定しておき、処理装置が記憶領域をアクセスするときには、PSW内のキーとアクセスの対象となる記憶領域に割り当てられているキーとを比較することにより、記憶領域の保護を行う。

第1図(a)は、PSWのビット構成を示すもので、2語64ビットのうちビット8～11に、保護キーと比較して記憶保護を行うアクセス・キーKEYが格納されている。

第1図(b)は、主記憶装置における保護キーの格納状態を示すもので、主記憶装置は一定バイト（例えば2048バイト）ごとのブロックに分割され、各ブロックに対して第1図(b)に示す保護キーKEYが設けられる。

(3)

ユーザとのプログラムアドレス0～2が格納されている領域には、それぞれ“0”以外の異なるキー“1”, “2”, “3”が割り当てられ、一方、PSWのアクセス・キーとしては、0Sが実行されるときにはキー“0”が、またユーザ・プログラムアドレス1, 2が実行されるときには、それぞれの領域と同一のキーが割り当てられる。処理装置のキーがキー“0”的プログラムは、どの領域にもアクセスできるので、システムを管理するプログラムはユーザ・プログラムへのアクセスが可能である。

このように、従来の記憶保護方式では、前述の第2段階で使用した論理アドレスの記憶領域を一定区画に分割して、分割された区画ごとに、例えばリング・レベル、アクセス権、記憶保護キー等の保護キーを与え、一方、命令実行時に前述の第1段階で使用したベース・レジスタとは別個に、例えばPSWにリング・レベル、記憶保護キー、等のアクセス・キーを与える。そして、これら2つの要素（キー）の関係で、記憶保護を行っている。

つまり、従来の記憶保護は、アクセス先記憶区

特開昭57-6952(2)
すなわち、ビット0～3は、対応するブロックに情報の読み出しと書き込みを行うとき、PSWのアクセス・キーKEYと一致しているかを比較するアクセス保護ビットKEYであり、ビット4は、記憶保護を書き込みだけ「0」、または読み書き「1」に適用する読み出し保護ビットである。

処理装置から主記憶装置がアクセスされるとき、PSWのアクセス・キーKEYと、主記憶装置の各ブロックごとの保護キーKEYとが比較され、例えば保護キーのKEYとFおよびアクセス・キーKEYの内容により第1図(d)に示すような制御が行われる。

第1図(d)では、各条件(OND)において、読み出し(RD)と書き込み(WT)が許可されるときOK、許可されないときNOで示されている。

これらのキーの割り当ておよび比較照合は、オペレーティング・システム(OS)の制御のもとで行われる。例えば、第1図(d)に示すように、ソフトウェアの基本的な働きを行うOSが格納されている領域にはキーKEY“0”が、またその下でエ

(4)

画と、アクセス命令の存在する記憶区画の各々に付与された保護情報の関係を照合することにより行われている。

しかし、これら2つの要素間の関係による保護方式は、プログラムあるいはプログラム集合体等の命令集合を単位として保護を行うものである。つまり、PSWはあるプログラム内のブロックごとに書き替えられ、その度にアクセス・キーが書き込まれるので、集合単位で記憶の保護が行われる。

したがつて、次のような欠点がある。

- (1) アクセス権情報（アクセス・キー）を管理するプログラムを作成しようとしても、どのようなプログラム単位に、またどの区画に対するアクセス権情報を与えればよいかを定めることができないため、有効な管理プログラムの作成が困難である。
- (2) プログラム作成者は、アクセス対象の保護情報（保護キー）を知り、アクセス権情報を制御しなければならないため、プログラミング時の負担が大きく、作成されたプログラムに誤りが生じ易い。
- (3) 一定区画ごとに保護情報が割り当てられていて

(5)

-284-

(6)

も、その区間に異なる種類の情報が格納されている場合には、情報との保護が行われない。また、プログラムが処理する情報との大きさに合わせた保護を行うためには、複雑な管理プログラムあるいは配慮領域に異なつた大きさの区画を設ける必要があり、処理能力も低下しやすい。

いま、ある領域 α がプログラム α とプログラム β とで共用され、プログラム α は別の領域 β にもアクセスするときのように、2つのプログラムが複数の異なる領域にアクセスする場合、保護を行うためには、アクセス領域を変更する度ごとに、アクセス・キーを変更する手続きを要求する必要があり、これを避けるためには、あらかじめそのプログラムに対して、アクセスする可能性のあるすべての領域の保護キーに対応した有効なアクセス・キーを付与する必要がある。

このように、従来の記憶保護方式では、保護される単位が大きくなる傾向にあり、厳密な保護を行い難く、しかも保護キーの管理に加えてアクセス・キーの制御が複雑である。

(7)

ツクのときには、ベース・アドレスは1個でよいが、分散した複数個のプロツクから構成されるときには、その数だけのベース・レジスタが必要である。

プログラムのためのベース・アドレスは、プロセッサー・ベース・アドレスと呼ばれる。ベース・レジスタが主記憶装置の最大容量まで表現できるビット数を持つていれば、命令語の番地部（ディスプレイスメント）は短いビット数でも主記憶装置のすべてをアドレスできるので、命令語の短縮が可能である。

本発明では、第2図に示すように、ベース・アドレス α がロケーション成分 β とアクセス・キー γ から構成されており、これらが一体として取り扱われる。なお、ロケーション成分 β とアクセス・キー γ の配置が逆の場合でもよい。

第3図は、本発明のベース・アドレスを用いて、実効アドレスを生成する過程の説明図である。

ベース・アドレス α は、ベース・レジスタ α に格納されている。また、命令 β は、命令コード β 、

本発明の目的は、このような欠点を除去するため、情報に対しアクセスを許可するプログラムの範囲を厳密に制限し、かつアクセス時およびアクセス権情報付与時の処理を簡単にできる記憶保護方式を提供することにある。

本発明の記憶保護方式は、命令で示すベース・アドレスとして、アクセス領域の位置を示すロケーション情報の他に、アクセス・キーを付加し、両者を一体として扱うことにより、保護情報の存在を意識することなく、命令単位で領域外へのアクセスを制限するようにしたことを特徴としている。

以下、本発明の実施例を、図面により説明する。

第2図は、本発明のベース・アドレスの構成を示す図である。

ベース・レジスタの中にプログラムのベース・アドレス（番地の基準となる番地）を格納し、命令語の番地にこの番地を加算すれば、絶対アドレスが得られる。プログラムを移動するときには、番地の変化分だけベース・レジスタの値を調整すればよい。プログラム全体が連続した1個のプロ

(8)

レジスタ番号 α_1 、インデックス・レジスタ番号 α_2 、ベース・レジスタ番号 α_3 、ディスプレイスメント α_4 から構成されている。

命令 β により指定したベース・レジスタ α の内容と、命令 β により指定したインデックス・レジスタ α の内容（偏差）と、命令 β 中に保持する偏差 δ との和をとつて、アクセス対象の実効アドレス α のアドレス成分 β を生成する。生成されたアドレス成分 β とベース・アドレスのアクセス・キー γ とから、実効アドレス α が求められる。

第4図は、本発明の実効アドレスのアドレス成分が論理アドレスのときの保護情報チェック動作の説明図である。

先ず、実効アドレス α のアドレス成分 β のセグメント番号 (B) より、セグメント・テーブル（S T） $1 \sim 3$ を参照してページ・テーブル・アドレスを読み出し、このセグメントのページ・テーブル（P T） $1 \sim 4$ を得る。次に、アドレス成分 β のページ番号 (B) より、ページ・テーブル $1 \sim 4$ のエントリを得る。

(9)

のと、一致関係に基づくものとがある。

第5図は、本発明の実施例を示すメモリ分割区画の要求とベース・アドレスの受渡し処理の説明図である。

キーの一貫性によりチェックする方式を用いる要求元プログラム18から管理プログラム17に対して、記憶領域の分割区画要求19があると、管理プログラム17は、ステップ21～23で分割区画を行つて保護キーを生成した後、これらを管理テーブル16のエントリーに登録し、ステップ24でアクセス・キーを生成して、要求元プログラム18に対してベース・アドレスの通知20を行う。

すなわち、記憶領域の分割区画の要求19に対して、管理プログラム17は、与える区画の先頭アドレスをロケーション成分2とし、あるログックにしたがつてキーを生成してそれを保護キー15とした後、保護キー管理テーブル(XPT)16の与える区画に対応するエントリーに登録する。一方、このキーをアクセス・キー3として、ペー

(11)

ス・アドレス1を生成し、ベース・アドレス1を要求元プログラムに通知する。

この分割区画にアクセスするプログラムは、記憶領域の管理プログラム17より通知されたベース・アドレス1を使用して、第3図に示す命令7のように使って実効アドレスを生成し、アクセスを行う。

次に、キーの生成について、説明する。

このようなベース・アドレス1に付与されたアクセス・キーは、隣接する区画に対する実効アドレスを不連続にする作用と、同一区画の用途が変更された場合に、旧実効アドレスを無効にする作用を持つ。したがつて、キーの作成には、論理的な時間経過とともに変化する値を使用することが最も望ましい。これは、タイマーの値から生成する方法や、領域要求の割り当てごとにカウント・アップするサイクリック・カウンタを利用することにより簡単に実現することができる。

いま、第5図において、プログラム18がユーザAのプログラムAであり、その他にユーザBの

(12)

プログラムBが存在するものと仮定する。先ず、プログラムAが記憶領域を要求すると、管理プログラム17からベース・アドレスa+d1(アクセス・キーは例えば805)で示される区画エリア0が与えられ、プログラムAはその区画エリア0を使用した後、管理プログラム17に返却する。

次に、プログラムBが記憶領域を要求すると、管理プログラム17からベース・アドレスa+d2(アクセス・キーは例えば910)で示される区画として、プログラムAが返却した区画エリア0が与えられたものとする。この場合、アドレスa+d1とa+d2はキーが異なるため(805と910)、プログラムAにバグがあり、プログラムAが区画0に対しベース・アドレスa+d1を使ってアクセスしても、本発明のチェック機構により検出され、プログラムBが使用している区画0の情報は保護される。

このように、ベース・アドレスの作成は、言語処理プログラムや管理プログラムの領域割り付け時に実施されるので、このアドレスを用いるプロ

(13)

-286-

(14)

グラムは、何らベース・アドレスの構成要素を意識することがない。

なお、このようなアドレス構造の情報処理システムでは、情報収集プログラムのようなデータ構造を無視して動作したいプログラムのために、保護キーのチェック回路を無効とするスイッチを備えるとともに、その操作命令も設けることができる。

本発明の記憶保護方式では、(1)記憶領域の分割区画を利用するプログラムは、保護情報の存在を意識することなく、領域のアドレスとしての意識のみでよいため、プログラムの作成がきわめて簡単となる。(2)キーの値として、時系列的な値を付与すると、時間的に領域に対するアクセスを制限できるため、使用済で管理プログラムに返却した区画に対して、プログラム内のバグによつて再返却したり、あるいは再アクセスすることを防止することができ、厳密な保護が可能である。

(3)プログラム間の情報の授受および共用は、情報格納領域アドレスの授受を介して行われるため、プログラム間で情報の授受、共用が行われると、

(15)

より、所有者は使用権を放棄し、譲り受けた側のみが使用権を持つことになるが、その場合、譲渡機能マクロ（プログラム）を作成して、そのプログラムによりキーを変更して、新しいベース・アドレスとして再割り付けを行えば、機密保護が簡単かつ厳密にできる。例えば、AプログラムからBプログラムに対しある区画エリア①を譲渡した後、Aプログラムで区画エリア①にアクセスしても、キーが変更されているため、チェックされて書き込みあるいは読み出しが不可能となり、機密が漏洩されない。

(7)ベース・アドレスを動作プログラムのプロセッサー・ベース・アドレスとして使用する場合、ブランチ等の制御の移行する範囲の検査にキーを使用できるので、きわめて有効である。

以上のように、本発明によれば、キー情報と記憶領域の先頭アドレス情報を一括して記憶領域のアドレスとして扱い、記憶領域側の区画に割り付けたキー情報と比較するので、アクセスを許可するプログラムの範囲を厳密に制限することができ、

保護情報も同時に授受されることになり、プログラム間を越えた保護も簡単に実現できる。

(4)従来は、プログラム内のユーザ領域ごとに書き替わられるPROMアドレス・キーが含まれていたが、本発明では命令で指定するベース・アドレスにアドレス・キーが含まれているため、命令単位にアドレス・キーを書き替えることができ、したがつて命令単位に区画エリア外へのアクセスを制限して、厳密な保護を行うことができる。

(5)実効アドレスによつて示される空間が、ベース・アドレス内のキー情報により見掛け上拡大されることになり、誤まつた実効アドレスに対応する論理アドレスが存在する確率を十分小さくできるため、ベース・アドレスの設定誤りに対しても十分な保護が可能となる。例えば、ベース・アドレスのロケーション成分を16ビット、アクセス・キーを4ビットとすると、誤まつた実効アドレスに対する確率は従来 $1/2^{16}$ であるのに対して、本発明では $1/2^{20}$ となり、十分に小さくなる。

(6)他プログラムへ領域の使用権を譲渡することに

(16)

かつアクセス時およびアクセス権情報付与時の処理を簡単にする等、種々の効果を与える。

4. 図面の簡単な説明

第1図は従来の記憶保護方式の一例を示す説明図、第2図は本発明の実施例を示すベース・アドレスの構成図、第3図は本発明によるベース・アドレスを用いて命令から実効アドレスを生成する過程の説明図、第4図は第3図による実効アドレスが論理アドレスのときの保護キー格納制御棟と保護キーのチェック動作の説明図、第5図は本発明によるメモリ分割区画の要求とベース・アドレスの受渡しの処理を示す図である。

1：ベース・アドレス、2：ロケーション成分、3：アクセス・キー、4：ベース・レジスタ、5：ディスプレイスメント、6：インデックス・レジスタ、7：命令、8：実効アドレスのアドレス成分、9：実効アドレス、10：セグメント番号、11：ページ番号、12：ミニページ番号、13：セグメント・テーブル(S.T.)、14：ページ・テーブル(P.T.)、15：保護キー、16：保護

(17)

—287—

(18)

キー登録制御表 (XPT)、17：管理プログラム
 △、18：要求元プログラム、19：分割区画要求
 求、20：ベース・アドレス通知。

特開昭57-6952(6)

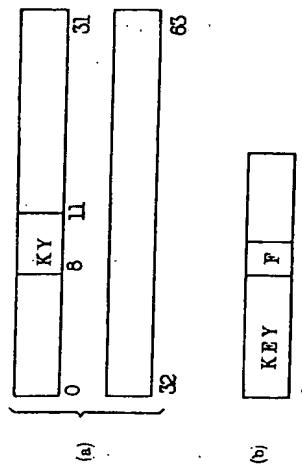
特許出願人 日本電信電話公社

代理人弁理士 矢村 雅

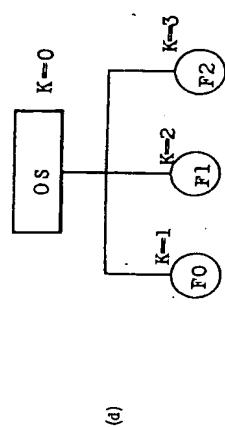


(19)

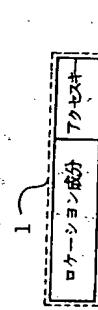
第1図



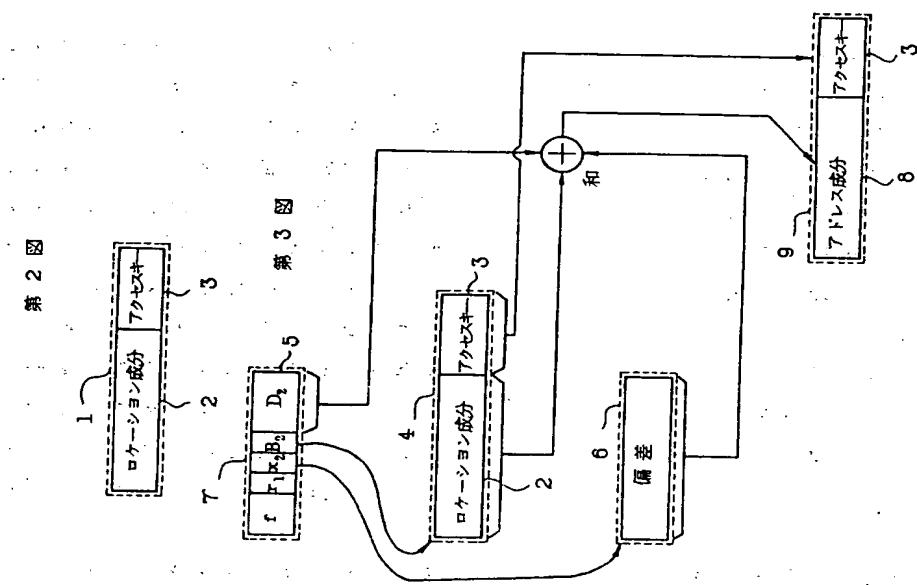
条件		RD	WT
KY=0	KEY, Fは無関係	OK	OK
	F=0 F=1	OK OK	OK OK
KY≠0	KEY	F=0 F=1	NO NO
	KY≠KEY	OK NO	NO NO



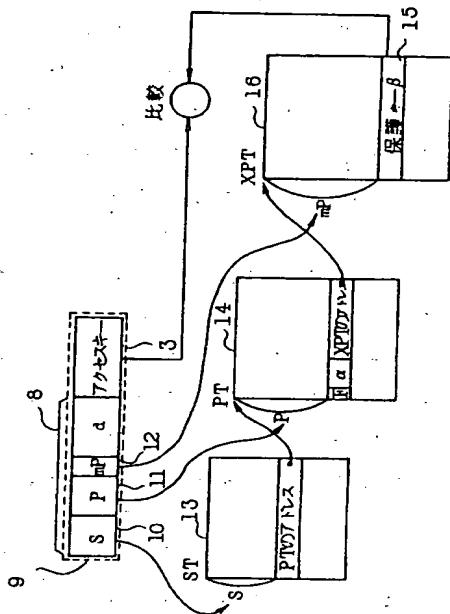
第2図



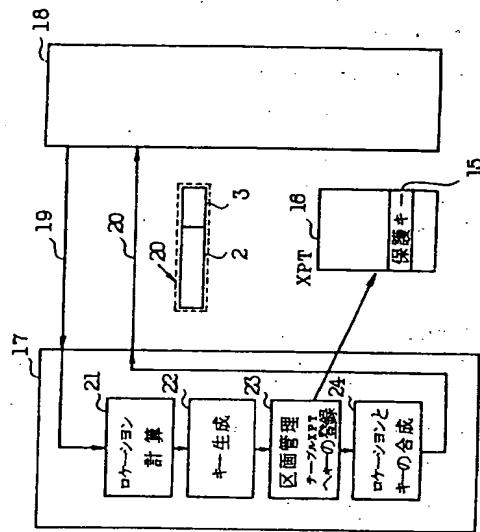
第3図



第4図



第5図



手続補正書（自発）

昭和56年2月12日

特許庁長官 島田春樹 殿 適

1. 事件の表示

昭和55年特許願第81157号

2. 発明の名称 記憶保護方式

3. 補正をする者

事件との関係 特許出願人

住所 東京都千代田区内幸町1丁目1番6号

名称 (422) 日本電信電話公社

代表者 真藤 信

4. 代理人

住所 東京都新宿区西新宿7丁目10番10号

西村ビル7階

氏名 (7727) 弁理士 磐村 雅

5. 補正により増加する発明の数 なし

6. 補正の対象 明細書および図面

7. 補正の内容 別紙の通り

(5) 明細書第10頁10行の「...求められる。」と11行の「第4図は、本発明の...」の間に、次の文章を挿入する。

「この様に生成された実効アドレスの前部のベース・アドレス1のアクセス・キー3に対応する部分をキー成分21として扱い、後部をアドレス成分8として扱う。

この実施例では、アクセス・キー3がアドレス演算の対象となつてゐるが、この演算の結果アクセス・キー3とキー成分21とが異つてしまふケースでも記憶域に割付けられた保護キーと、このキー成分21とが一致する事は少ないので、両者の一致関係でチェックする方法を用いれば、問題はない。第3-1図は、アクセス・キー3をアドレス演算の対象としない本発明のベース・アドレスを用いて実効アドレスを生成する過程の説明図である。

ベース・アドレス1は、ベース・レジスタ4に格納されている。また、命令7は、命令コード r_1 、レジスタ番号 R_1 、インデックス・レジスタ番号 E_1 、

(1) 明細書第1頁の「特許請求の範囲」の欄の記載を次のとおりに補正する。

「記憶領域を画面に分割し、該画面ごとに保護キーを割り当てるとともに、該記憶領域にアクセスする命令がベース・アドレスの格納場所を指定するような情報処理装置において、該ベース・アドレスがロケーション成分とアクセス・キーで構成され、実効アドレスのアドレス成分をもとにして、記憶領域に割り当てられた保護キーを得、該保護キーと実効アドレスに示されるキー成分とを比較チェックすることを特徴とする記憶保護方式。」

(2) 明細書第9頁15行～16行の「なお、ロケーション成分2と...よい。」を削除する。

(3) 明細書第10頁7行～8行の「アクセス対象の実効アドレス9のアドレス成分8を生成する。」を「アクセス対象の実効アドレス9を生成する。」に補正する。

(4) 明細書第10頁8～10行の「生成されたアドレス成分8とベース・アドレスの...が求められる。」を削除する。

(1)

ベース・レジスタ番号 B_1 、ディスプレイスメント D_1 から構成されている。

命令7により指定したベース・レジスタ4の内容と、命令7により指定したインデックス・レジスタ6の内容（偏差）と、命令7中に保持する偏差5との和をとつて、アクセス対象の実効アドレス9のアドレス成分8を生成する。生成されたアドレス成分8とベース・アドレスのアクセス・キー3とから、実効アドレス9が求められる。

このように、実効アドレス9の生成において、キー成分21を分離して扱う事は、第3図に示した実施例に比して次の効果がある。

(1) インデックス・レジスタの加算により生じたアドレス成分の桁^上を^上検出でき、より厳密に記憶保護を行うことができる。

(2) アクセス・キー3の内容がキー成分21として保存されるので、より厳密に記憶保護を行うことができる。

(3) キー成分21を保持する金物をアクセス・キー3を保持する金物で代用する事が可能であり、

(3)

金物を削減することができる。なお、本実施例では、ロケーション成分2とアクセス・キー3の配置が逆の場合でもよい。」

(6)明細書第11頁17行の「アクセス・キー3」

および同第11頁19行の「アクセス・キー3」を、いずれも「キー成分21」に補正する。

(7)同第13頁5行の「第3図に示す命令7」を「第3図または第3-1図に示す命令7」に補正する。

(8)同第18頁6行の「第3図は本発明による...」を「第3図および第3-1図はそれぞれ本発明による...」に補正する。

(9)同第18頁8行の「第3図による実効アドレス」を「第3図および第3-1図による実効アドレス」に補正する。

(10)同第19頁3行の「求、20：ベース・アドレス通知」を「求、20：ベース・アドレス通知、2.1：実効アドレスのキー成分。」に補正する。

(11)第2図を別添の第2図に補正する（差し替え）。

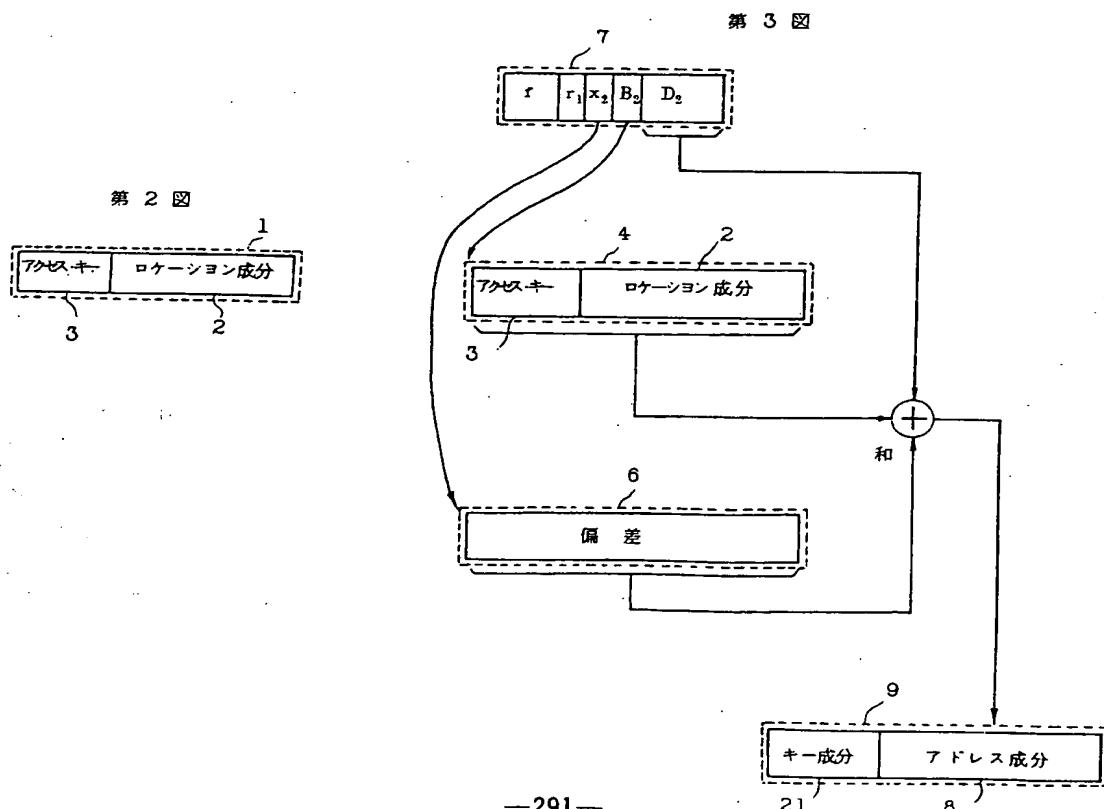
(12)第3図を別添の第3図に補正する（差し替え）。

(13)第3図の次に別添の第3-1図を追加する。

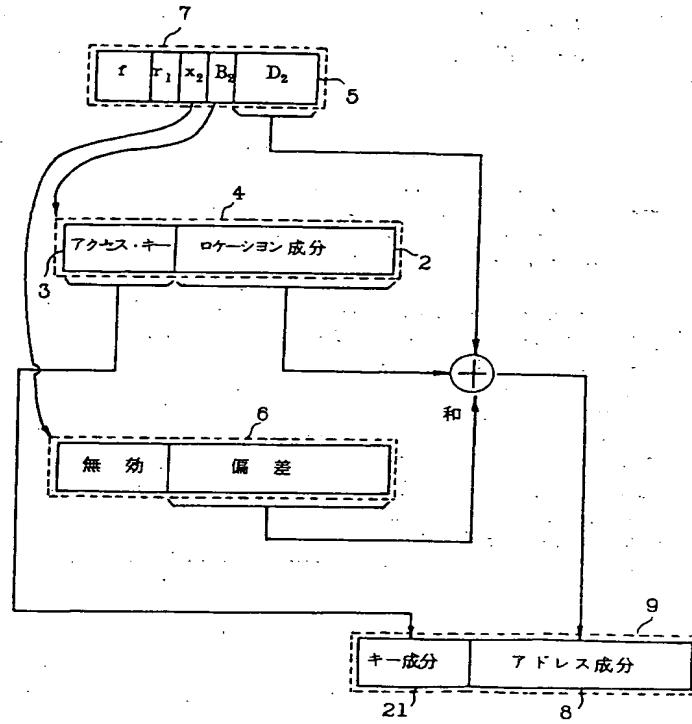
(14)第4図を別添の第4図に補正する（差し替え）。

(4)

(5)



第3-1図



第4図

